BILL ANALYSIS

Senate Research Center
86R22664 KSM-F

C.S.S.C.R. 21
By: Kolkhorst
Health & Human Services
4/2/2019
Committee Report (Substituted)

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

On June 11, 2015, the Department of Aging and Disability Services (DADS), a "covered entity" under Privacy, Security, and Breach Notification Rules (HIPAA Rules), filed a breach notification report with the United States Department of Health and Human Services, Office for Civil Rights (OCR) stating that an impermissible disclosure of unsecured electronic protected health information (ePHI) in violation of HIPAA Rules had occurred when a DADS web application was accessible to unauthorized parties.

On July 23, 2015, OCR notified DADS of its investigation of DADS compliance with the HIPAA Rules and determined that:

a. DADS failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity. (See 45 C.F.R. Section 164.308(a)(1)(ii)(A));

b. DADS failed to implement appropriate technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 45 C.F.R. Section 164.308(a)(4). (See 45 C.F.R. Section 164.312(a)(1))

c. DADS failed to implement appropriate hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contained or used ePHI. (See 45 C.F.R. Section 164.312(b));

d. As a result of its failure to appropriately safeguard the ePHI in a web-based application, DADS impermissibly disclosed the ePHI of up to 6,617 individuals. (See 45 C.F.R. Section 164.502(a)); and

OCR presented the State of Texas a Resolution Agreement with Corrective Action Plan (the "Settlement Agreement") in lieu of civil monetary penalties and to provide DADS an opportunity to correct DADS ’s failures to safeguard ePHI.

The State of Texas has presented a counter-proposal to the Settlement Agreement to OCR that applies to those covered functions and information resources involved in the breach that were formerly operated by DADS but that have been transferred to the Health and Human Services Commission (HHSC).

The proposed Settlement Agreement comprises the following terms and conditions:

Payment. HHSC agrees to pay the amount of $1,600,000.00.

Corrective Action Plan. HHSC has entered into and agrees to comply with a Corrective Action Plan ("CAP"). If HHSC breaches the CAP, and fails to cure the breach as set forth in the CAP, then HHSC will be in breach of the Settlement Agreement and OCR will not be subject to the release set forth in the Settlement Agreement. Compliance with the RA/CAP of the Settlement Agreement by HHSC is conditioned upon HHSC obtaining the approval of, and appropriation of funds needed to comply with, the RA/CAP by the Legislature of the State of Texas. (See Texas Civil Practice and Remedies Code Section

111.003(b)). The term of the CAP will be three (3) years from the effective date of the proposed agreement.

Release by OCR. In consideration of and conditioned upon performance by HHSC of its obligations under the proposed Settlement Agreement, OCR releases HHSC from any actions it may have against HHSC under the HIPAA Rules arising out of or related to the conduct identified in paragraph 2 of this concurrent resolution. OCR does not release HHSC from, nor waive any rights, obligations, or causes of action other than those arising out of or related to said conduct and referred to in this paragraph.

Agreement by Released Parties. HHSC shall not contest the validity of its obligation to pay, nor the amount of, the Resolution Amount or any other obligations agreed to under the proposed Settlement Agreement. HHSC waives all procedural rights granted under Section 1128A of the Social Security Act (42 U.S.C. Section 1320a-7a); and 45 C.F.R. Part 160, Subpart E; and claims collection regulations at 45 C.F.R. Part 30, including, but not limited to, notice, hearing, and appeal with respect to the Resolution Amount.

Section 111.003(a)(2), Civil Practice and Remedies Code, requires the legislature to approve a settlement of a claim or action against the state if the settlement commits the state to a course of action that in reasonable probability will entail a continuing increased expenditure of state funds over subsequent state fiscal biennia.

The CAP of the proposed agreement commits the State of Texas to a course of action that in reasonable probability entails a continuing increased expenditure of state funds over subsequent state fiscal biennia.

RESOLVED

That the 86th Legislature of the State of Texas approve the proposed Settlement Agreement.